SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks 2014; **7**:2114–2124
Published online 10 January 2014 in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.923

RESEARCH ARTICLE

Security risk assessment framework for cloud computing environments

Sameer Hasan Albakri, Bharanidharan Shanmugam*, Ganthan Narayana Samy, Norbik Bashah Idris and Azuan Ahmed

Advanced Informatics School, Universiti Teknologi Malaysia, Malaysia

ABSTRACT

Cloud computing has become today's most common technology buzzword. Despite the promises of cloud computing to decrease computing implementation costs and deliver computing as a service, which allows clients to pay only for what they need and use, cloud computing also raises many security concerns. Most popular risk assessment standards, such as ISO27005, NIST SP800-30, and AS/NZS 4360, assume that an organization's assets are fully managed by the organization itself and that all security management processes are imposed by the organization. These assumptions, however, do not apply to cloud computing environments. Hence, this paper proposes a security risk assessment framework that can enable cloud service providers to assess security risks in the cloud computing environment and allow cloud clients to contribute in risk assessment. The proposed framework provides a more realistic and accurate risk assessment outcome by considering the cloud clients' evaluation of security risk factors and avoiding the complexity that can result from the involvement of clients in whole risk assessment process.

KEYWORDS

cloud computing; cloud computing security; information security risk assessment framework

***Correspondence**

Bharanidharan Shanmugam, Advanced Informatics School, Universiti Teknologi Malaysia, Malaysia.
E-mail: bharani.kl@utm.my

1. INTRODUCTION

Since the inception of the term "cloud computing" as introduced by Googles CEO Eric Schmidt in 2006 [1], numerous studies had been conducted on this subject. The terminology and its related technology has improved rapidly ever since. According to the National Institute of Standards and Technology (NIST), the important characteristics of cloud computing include on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Three main service models exist: software as a service (SaaS), where the consumer controls only the application configurations; platform as a service (PaaS), where consumers can control only the hosting environment; and infrastructure as a service (IaaS), where the consumer controls everything except the data center infrastructure. Cloud computing also has four main deployment models: public, community, private, and hybrid clouds [2].

The cloud computing model has many economic and functionality advantages especially for small and medium-sized businesses. Low cost, availability of resources, energy savings, and increased focus on business objectives are some of its economic benefits. Consolidation, efficient configuration and management, elastic scaling, resource pooling, broad network access, and on-demand self-service are important cloud computing advantages that affect the system's functionality and performance [3,4]. Cloud computing providers are able to build large data centers at low cost, organize and provide computing resources, and achieve efficient resource utilization [3,5]. Company decision makers share many concerns about cloud computing environment, in particular, data security being on the forefront [6]. Surveys conducted by the International Data Corporation (IDC) Enterprise Panel in 2008 and 2009 showed that Chief Information Officers (CIOs) consider confidentiality, availability, and reliability as primary concerns [4]. Similarly, 70% of the respondents in a survey from Japan conferred their concerns on the security in cloud computing [7]. In addition, the European Network and Information Security Agency conducted a survey of small and medium-sized businesses, which confirmed that their major concern on cloud computing included data confidentiality and liability for incidents that involved the infrastructure [4,5].

The security concern has different levels in the different deployment model of cloud computing, due to the difference levels of trust among the communicating parties of each model. The trust in the private cloud computing model is expected to be at the highest level as the infrastructure and the assets will be managed and used by specific and well-known entities. In the community cloud computing model, the cloud clients (CCs) are from different organizations, they will have the same level of security requirements. The trust level here may be lesser than the trust level in the private cloud, yet it is still better than the public cloud model. In fact, the real problem of trust is in the public cloud computing model, in which the communication entities are unknown to each other. However, it is the service providers responsibility to build trust with its clients. Cloud service providers with security certificate such as ISO27001 enhance its credibility and confidence to its CCs.

In fact, most popular risk assessment standards, such as ISO27005, NIST SP800-30, and AS/NZS 4360, assume that an organization's assets exist within that organization's data center and are fully managed by the organization itself and that security management processes are determined by the organization itself [8,9]. However, the characteristics of the cloud computing model invalidate this assumption [6].

In the cloud computing model, data assets will be moved to the data center of the cloud service provider. The dilemma in this case is that the CC will not be able to assess the security system of the service provider. Conversely, the service provider Cloud Service Provider (CSP) will not provide extensive details on its security system to hinder hackers who may be doubling as clients. Some researchers have suggested that both the service provider and CC should depend on a trusted third party to assess the security system of the service provider. However, the main problem here lies in the risk assessment process itself. One of the most important step in the conventional risk assessment process is defining the risk criteria. Risk criteria are defined according to the organization's business objectives, and this is then used to evaluate the level of risks, based on which risk treatment plan will be established. Thus, regardless of who conducts the risk assessment process, risk criteria are defined according to the business objectives of the service provider and not those of the client. However, it must be noted that the CC is the real owner of the data assets and is the only one who knows the real value of the data and the realistic consequences of data security breaches. Thus, ignoring the client's business objective will result in an inaccurate evaluation of security risk level. On the other hand, if the service provider involves the clients in all risk assessment steps, the risk assessment process will become very complicated and difficult to manage. Thus, security risk assessment in cloud computing requires further research to develop an appropriate risk assessment methodology. An ideal risk assessment methodology must be capable of considering the CC's business objectives without involving the CC in all stages of the risk assessment process to minimize complexity.

This paper proposes a security risk assessment of the cloud computing environment by considering both the CC and the CSP during its risk assessment process. We believe that more accurate result can be obtained and more comprehensive risk evaluation can be made by considering both the CCs and the CSP. The proposed framework defines the responsibilities of the different stakeholders (i.e., the CSP and the CCs) during security risk assessment. Although the proposed framework is aimed at public cloud computing, it is still viable to be used in other models such as the community and hybrid model.

This paper is organized as follows. The next section briefly describes the most popular security risk assessment standards and guidelines. Section 3 reviews some existing research efforts to assess security risk in cloud computing environments. The proposed framework is presented in Section 4. Section 4.7 discusses an initial experiment using the proposed framework. The conclusion is given in the final section.

2. INFORMATION SECURITY RISK ASSESSMENT APPROACHES

No one can guarantee hundred percent on the security of information systems. However, the efficient and effective information security risk assessment method can provide high-level of confidence for the CCs [10]. There are many information security risk assessment methods, standards, and regulations such as NIST SP800-30, International Organization for Standardization (ISO) 27005, Australia Standards and New Zealand Standards (AS/NZS) 4360, and Control Objectives for Information and Related Technology (COBIT). They are released by governmental and private organizations such as the NIST and the ISO. In the succeeding text is a brief summary of some of the security risk assessment standards that is used in the conventional information systems. These standards can be modified in some of its application to suit the cloud computing environment.

2.1. National Institute of Standards and Technology Guidelines

The NIST is a US governmental organization. NIST introduces guidelines that are to be used by federal organizations, which process sensitive information. NIST's guidelines may also be used by non-governmental organizations. NIST released a special publication (SP) 800–30 in 2002 titled "Risk Management Guide for Information Technology Systems". The NIST in this guide introduced a risk assessment methodology that encompass nine primary steps: system characterization, threat identification, vulnerability identification, control analysis, likelihood determination, impact analysis, risk determination, control recommendations, and results documentation. In

September 2011, NIST published the draft of the first revision of SP 800–30. The updates of SP 800–30 focused on risk assessments, one of the four steps in the risk management process. The revision provided in-depth insights on the essential factors of risk (e.g., threat sources and events, vulnerabilities and predisposing conditions, impact, and likelihood of threat occurrence) that influenced information security risk determinants [11]. However, in March 2011, NIST considered the SP 800–39 "Managing Information Security Risk Organization, Mission, and Information System View", a publication that was considered as a big umbrella for NIST risk management guidelines such as the SP 800–30 guideline. The SP 800–39 provided comprehensive information security risk management guidance for organizations. It covered the organizations operations (i.e., mission, functions, image, and reputation), assets, individuals, other organizations, and the nation with the operation and use of federal information systems [12].

2.2. The International Organization for Standardization Standards

The ISO is a non-governmental international body that collaborates with the International Electrotechnical Commission (IEC) and the International Telecommunication Union on information and communications technology standards. The following are commonly referenced to as ISO security standards: ISO/IEC developed a family of standards known as "Information Security Management System Standards" or "27000 Family of Standards", ISO/IEC 27000 "Information Security Management Systems—Overview and vocabulary", ISO/IEC 27001 "Information Security Management Systems—Requirements", ISO/IEC 27002 "Code of Practice for Information Security Management", ISO/IEC 27003 "Information Security Management System Implementation Guidance", ISO/IEC 27004 "Information Security Management—Measurement", ISO/IEC 27005 "Information Security Risk Management", and ISO/IEC 27006 "Requirements for Bodies Providing Audit and Certification of Information Security Management Systems". There are many other standards developed by ISO/IEC targeting the information security field. However, most of these standards were replaced or updated to one of the 27000 standards, such as ISO/IEC 17799:2005, that was replaced by ISO/IEC 27002. Moreover, some of the technical reports that were reviewed had superseded one of the 27000 standards, such as ISO/IEC TR 13335–3 and ISO/IEC TR 13335–4, that was superseded by ISO/IEC 27005 [13]. ISO/IEC 27005 standard is dedicated to information security risk management. For a complete understanding of ISO/IEC 27005, the concepts, models, processes, and terminologies described in ISO/IEC 27001 and ISO/IEC 27002 may be referred. ISO/IEC 27005 is applicable to manage risks in all types of organization. These standards have important value in its potential application in cloud computing security [14].

2.3. Australia Standards and New Zealand Standards 4360 standard

Australia Standards and New Zealand Standards 4360:2004 is a general risk management guide; it can be applied to all forms of organizations. The AS/NZS 4360 risk management process contains three major elements: risk management workflow, monitor and review, and communication and consultation.

2.4. Control Objectives for Information and Related Technology

Control Objectives for Information and Related Technology provides a comprehensive control framework that links IT initiatives to business requirements and enables enterprises to manage their information and technology assets (IT). COBIT, which was released for the first time in 1996, had its latest update version 5, published in April 2012. COBIT 5 is based on five key principles for the governance and management of IT enterprises: meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, enabling a holistic approach, and separating governance from management. The COBIT 5 framework describes seven categories of enablers: principles, policies and frameworks; processes; organizational structures; culture, ethics and behavior; information; services, infrastructure, and applications; and people, skills, and competencies [15].

3. SECURITY RISK ASSESSMENT IN CLOUD COMPUTING

The cloud computing model has certain unique characteristics and uses techniques that have raised several new risks and the need to reevaluate and redefine many well-defined past risks accorded to the model [6]. An extensive research effort was focused on defining cloud computing risks. Analyst firm Gartner published a 2008 report on cloud computing where it warned customers to select their cloud computing provider very carefully and to consider seven specific security issues: *privileged user access*, *regulatory compliance*, *data location*, *data segregation*, *recovery*, *investigative support*, and *long-term viability* [16]. On the basis of previous studies [4], 32 risks were identified, some new and some pre-existing [7]. Some studies on cloud computing saw risks from the clients' perspective and identified 23 risks. ENISA published its own report on cloud computing security risks, which estimated risk levels on the basis of the ISO/IEC 27005 standard, which were dependant on risk probability and risk impact. The ENISA report lists 35 risks, which were organized into three categories: policy and organizational risks, technical risks, and legal risks [17].

Numerous researchers have proposed risk assessment methods in the cloud computing environment. Some of these studies focused on specific security problems, such

as insider attacks, virtualization threats [18–21], data transmission with cloud computing [22] service-level agreement [23,24], anti-virus in the cloud service [25], denial of service attacks in cloud [26], and identity management [27]. In addition, frameworks, which are used to assess security risks in cloud computing environments as a whole process, have also been proposed. Those proposals varied on the basis of their study perspectives. Some studies proposed frameworks that can be used by the CC and even suggested transferring some risks to the CSP or to a trusted third party. Saripalli, P. and B. Walters presented a quantitative framework for analyzing and assessing the risks and impacts to the security of cloud-based software deployments. The US Federal Information Security Management Act defined three security objectives (SO) for information and information systems, as Confidentiality, Integrity and Availability. Saripalli and Walters have proposed addition of three more SO in the context of cloud platforms: multiparty trust, mutual auditability, and usability. These six SO for the cloud platforms are referred to as the CIAMAU framework. Establishing an appropriate security objective for each threat event requires determining its potential impact first. Impact always corresponds to a specific threat event e, which maps to one of the six SO such as Ie = [(C, 12), (I, 6), (A, 5), (M, 1), (A, 1), (U, 8)]. They depend on the expert opinions to estimate the impact of security incidents [4]. S. Tanimoto *et al.* [7] used the risk breakdown structure method to extract the risk factors in cloud computing from the users' viewpoint. They addressed three main subjects of security: *existence of two or more stakeholders, security guarantee in disclosure environment*, and *mission critical data problem*. Twenty-three risk factors were extracted and grouped into three major divisions: *risks for company introducing cloud, risks for cloud service provider*, and *others*. They used the decision tree analysis method to analyze and evaluate the extracted risk factors, which were dependant on the risk matrix. The risk matrix method classifies risks into four kinds (*risk avoidance*, *risk mitigation*, *risk acceptance*, and *risk transference*) in accordance with the generation frequency and degree of incidence.

However, these studies overlooked the fact that the CSP owns and manages the infrastructure of the cloud environment. Other proposed frameworks were designed to be used by the CSP to assess the risks in cloud computing [28,29].

Xuan *et al.* proposed an information security risk management framework that has seven processes, including processes selecting relevant critical areas, strategy and planning, risk analysis, risk assessment, risk mitigation, assessing and monitoring program, and risk management review. They assessed the risk from the cloud service provider's perspective [28]. Fito *et al.* [30] proposed a cloud risk management process led by business level objective (BLO) and a semi-quantitative BLO-driven cloud risk assessment as its core sub-process. Their proposed approach was based on Federation of European Risk Management Association's standard [31]. Their risk management processes framework contains *semi-quantitative BLO-driven cloud risk* assessment (i.e., risk assessment, risk analysis, and evaluation), *risk reporting and communication*, *risk treatment*, and *risk monitoring*. The model focuses only on evaluating the impact of cloud-related risks on BLOs. It is the core process of the BLO-driven cloud risk management and has risk level estimations as outputs, which are individually specified for each risk and BLO (*Bi*) affected. In risk assessment process, their model calculates the likelihood of occurrence of risk, and it estimated the positive (i.e., upside risks; opportunities) and negative (i.e., downside risks; threats) impacts on the BLOs. They use a 10×5 matrix, considering five possibilities for positive and the remaining five for negative impacts [30].

However, these frameworks had underestimated the importance of involving the CCs in the risk assessment process. The assessment of the CC must be considered because they know how data security violations can affect them. Still, the CC cannot be involved in the entire risk management process because the process becomes very complicated as the number of CCs increases. CC participation must be minimal and is necessary only for evaluating factors that affect the risk assessment results. In cloud computing, the physical infrastructure and sometimes the software used to process the data are owned by the CSP, whereas the data are owned by the CC, who alone knows the real consequences of losing data security. Thus, assessing the security risk from one side only leads to inaccurate risk evaluation. An ideal risk assessment methodology must be capable of considering the CC's business objectives without involving the client in all steps of the risk assessment process to minimize complexity.

Security responsibilities in the cloud computing model vary according to the service delivery models. Three distinct models exist: IaaS, PaaS, and SaaS. In the IaaS model, providers offer on-demand virtual machines, storage, or database services to clients. The client does not manage or control the underlying cloud infrastructure but can perform many activities on the server, including starting or stopping the server, installing software packages, adding virtual storage, and configurating the access permissions and firewall rules. In this model, the service provider will be responsible for the physical security and the security of the virtual machine manager, which is the program that manages all virtualization functions. Moreover, the service provider will be responsible for the security of the means of access used by clients to gain access to the offered resources. On the other hand, the client will be responsible for the security of the operating system that he installed as well as all software within his own operating system. Further, the client is also responsible for the virtual network configurations.

In the PaaS model, the PaaS provider offers multiple programming models as building blocks for new applications such as email and image manipulation services. The client is able to develop and deploy his own applications on the cloud without having to worry about the underlying infrastructure such as network, servers, operating systems,

or storage. In this model, the responsibilities of the service provider will be expanded to cover the operating system and the software infrastructure that manages client applications. The client will be responsible for data security within the applications that he had developed. Thus, the security responsibility of the client will decrease, whereas that of the service provider will increase. In the SaaS model, which is the most popular model, the client will use software that is owned, delivered, and managed remotely by one or more providers. However, customers may extend the data model by using provider configuration tools without altering the source code. The SaaS provider is responsible for software upgrades, maintenance, and security. Client responsibility will be at the minimum level, with the client only being responsible for the security of his own account. In brief, the responsibilities of each stakeholder is different in each cloud service model. The consequence of this is that the risk assessment framework that was designed for one cloud service model may not be appropriate for another model. Our model is designed to fit the SaaS model.

This paper proposes security risk assessment method for cloud computing environment by considering both the CC and the CSP during the risk assessment process. We believe that by combining both the CCs and the CSP, it ensures the most accurate result and is a more realistic risk evaluation method. The proposed framework defines the responsibilities of the various stakeholders in security risk assessment.

4. PROPOSED FRAMEWORK

In cloud computing environments, the CSP and the CCs must be involved throughout the risk assessment process. Some published frameworks, such as [8], suggest involving the CCs in all risk assessment processes. However, doing so, greatly complicates the risk assessment process, particularly when the number of the clients increases. Defining the appropriate level of CC participation in the risk assessment process is critical. Generally, risk decision is based on certain factors, such as asset value, the likelihood that a vulnerability has been exploited, and the severity of the impact of an incident [32]. In the proposed framework, we limit client inclusion to processes that define the security risk factors, such as asset value, likelihood of threat, vulnerability, and impact of the incident.

We reviewed some of the more popular security risk assessment methods, such as ISO27005, NIST SP800-30, and AS/NZS 4360, to determine the critical steps in security risk assessment. In this paper, we relied on the ISO27005 standard to define the main steps of the security risk assessment. ISO27005 divides the security risk management process into six steps: context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review. The proposed security risk assessment framework for cloud computing involves the inclusion of CCs, which guarantees the CCs' evaluation of the risk factors, which are considered during risk assessment. In fact, certain tasks of the CSP and the CCs overlap, hence blurring the distinction of their responsibilities in the overall security program. This overlap has different levels to suit in different cloud computing models. However, the present study is limited to the SaaS model only.

Although the client may define their security requirements through the service-level agreement, later modifications are obscure. The present framework aims to balance between realistic results that can be obtained from the contributions of CCs and the complexity that can be caused by the involvement of CCs in the risk assessment process. This framework provides a dynamic relationship between the CSP and the CCs, which enables the CSP to be more flexible and more knowledgeable about the status of the CC.

This paper proposes a framework that enables CCs to contribute to the risk assessment process by defining risk factors, which will therefore produce better and more realistic risk assessment results. On the hind side, the CSP will not be able to manage the risk assessment operation, if all clients are involved in each of the risk assessment step. Thus, this framework limits the contribution of the CCs to three tasks: defining legal and regulatory requirements, identifying security risk factors, and receiving feedback from the CSP and applying the required security tasks. This section discusses the steps in the risk assessment process and the tasks that must be completed by both the CSP and the CCs in each of this step.

Figure 1 depicts the proposed framework, which consists of two main parts (the CSP and the CCs) separated by dotted lines. The first part represents the CSP side, which contains four main entities: the risk assessment manager (cloud service provider risk assessment manager [CSPRAM]), the CC communicator (cloud service provider cloud client communicator [CSP3C]), the security requirements classifier (cloud service provider security requirements classifier [CSPSRC]), and the database interface (cloud service provider database interface). The second part represents the CCs, which contains one main entity, namely, the CC risk assessment assistance. The CSP uses the CSP3C to handle all communication between the CSP and CSs during the risk assessment process. The CSP3C relays received information from the CCs to the CSPSRC. The CSPSRC then categorizes this information and saves them in the database. The most important function of the CSPSRC is to make decisions on the security requirements and the importance of threats received from the CCs. The CSPSRC may make these decisions after receiving all information from the CCs. The CSPRAM is the CSP entity that is responsible for managing the risk assessment processes as a whole and sending feedback to the CCs. The CC risk assessment assistance is the CC entity that is responsible for communication between the CC and the CSP. Table I provides a summary of the abbreviations used in the proposed framework.

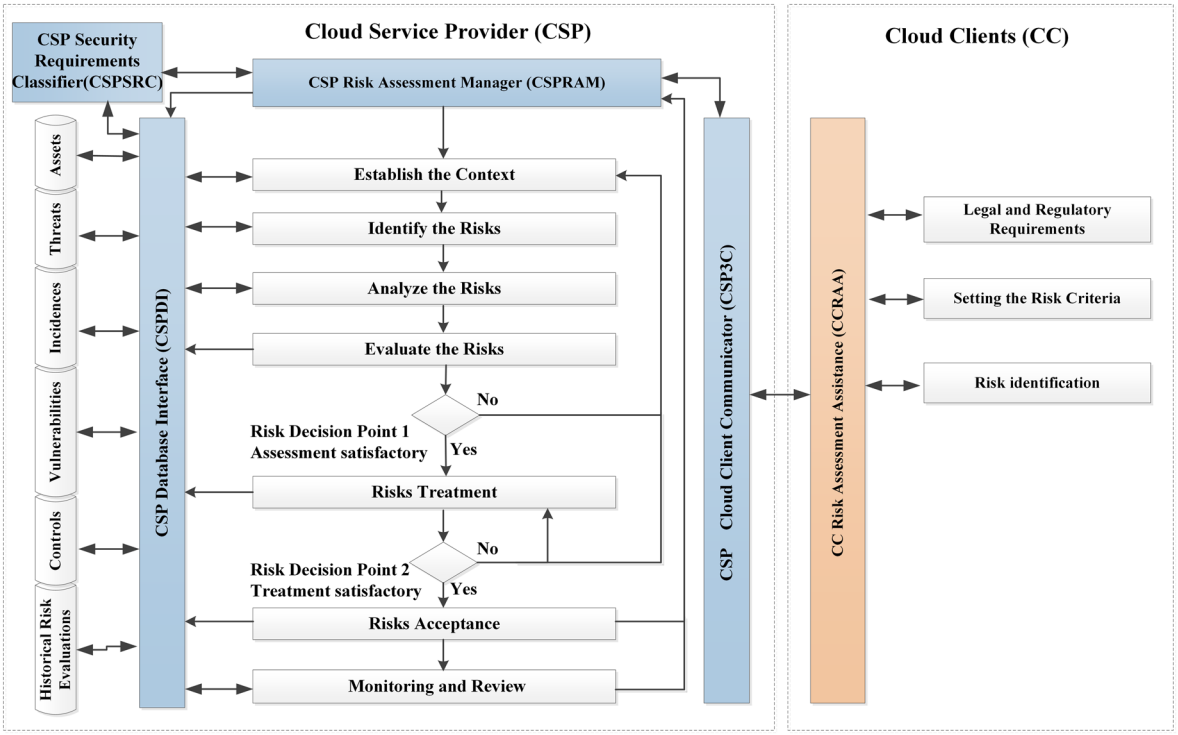

Figure 1. Proposed security risk assessment framework.

Table I. Abbreviation table.

Abbreviation	Meaning
CC	Cloud client
CCRAA	Cloud client risk assessment assistance
CSP	Cloud service provider
CSP3C	Cloud service provider cloud client communicator
CSPDI	Cloud service provider database interface
CSPRAM	Cloud service provider risk assessment manager
CSPSRC	Cloud service provider security requirements classifier
IaaS	Infrastructure as a service
PaaS	Platform as a service
SaaS	Software as a service

4.1. Context establishment

In traditional information systems, the external and internal context for information security risk management would be established during this step. The context establishment process consists of three sub-processes: setting the basic criteria, setting the scope and boundaries, and organizing the information security risk management process. Setting the basic criteria involves three types of criteria: risk evaluation, impact, and risk acceptance criteria. The impact criteria would determine the degree of damage or the consequences of the risk. The risk acceptance criteria are based on the organization's objectives and policies and the concerns of the stakeholders. The second sub-process of the context establishment process involves defining the scope and boundaries of the organization. This process aims to ensure that all relevant assets are taken into account in the risk assessment. The last sub-process of the context establishment process involves organizing the information of the security risk management process [33].

In our proposed cloud computing model framework, when the CSP decides to begin the risk assessment operation, the CSPRAM instructs all clients to send their information via CSP3C. Each CC that receives the CSPRAM notification must start its own context establishment process. The CC should assess the data that are moved (or are to be moved) to the CSP infrastructure to determine the legal compliance of the data. If the data are governed by certain laws, the CC must clearly report this fact to the CSP. Further, the CC should define their criteria for risk evaluation, risk impact, and risk acceptance according to their organization's business objectives, business operations, and the importance of their information assets. Here, the CSP would include the entire infrastructure (i.e., both hardware and software) during context establishment. The information received by the CSP from the CCs helps define the clients' constraints and determines its legal obligations. Moreover, the information from the CC helps the CSP set the basic criteria for risk assessment and properly organizes the information security risk management process. Thus, during the context establishment phase, the CSP considers the criteria and expectations of the CCs.

4.2. Risk assessment

Risk assessment is the most important step in security risk management and involves three main sub-processes, namely, risk identification, risk analysis, and risk evaluation. Risk identification covers the identification of assets, threats, existing controls, vulnerabilities, and consequences. Risk analysis or risk estimation consists of three sub-processes, namely, assessment of the consequences, assessment of incident likelihood, and the level of risk determination. The final output of risk assessment is a list of assessed risks prioritized according to the risk evaluation criteria [33].

The aim of risk identification is to answer the following questions: What caused the loss? How? Where? Why? Information on the assets, threats, existing controls, vulnerabilities, and consequences should be identified and gathered to answer these questions. The assets could be hardware or software owned and managed by the CSP and data owned by the CCs. The CCs know the consequences that will arise if their data security is compromised, hence justifying their involvement in risk identification.

In the cloud computing environment, the CSP will notify the CCs through the CSP3C to start the risk identification. Every CC will study the data that were moved to the cloud to determine the importance of the data and its impact on the objectives of the organization and business operations, to evaluate the assets according to their criticality, to identify threats that may attack the assets and the vulnerabilities that may exist on the CC's side and to review historical and expected incidents and the possible consequences. Each CC should submit the collected information to the CSPRAM through the CSP3C. However, the CSP may conduct its own risk identification (i.e., hardware and software assets). The CSP may classify the risk identification lists obtained from the CCs based on their security requirements. The CSP is responsible for integrating the CCs' identification lists and is required to study them before moving on to risk analysis and risk evaluation.

Assets: ISO27005 defines assets as "anything that has value for the organization." It considers information and business processes as primary assets and hardware, software, network, personnel, site, and the organization's structure as supporting assets. Generally, primary information may comprise personal information; vital information for business operations; strategic information required for achieving objectives determined by strategic orientations; and high-cost information of which, gathering, storing, processing, and transmitting require a long time and/or high acquisition cost [33]. However, this study distinguishes assets that may be under the CSP's control from those that are not. The CC's assets that must be identified and passed to the CSP are the software assets (i.e., data, any extension of the applications developed by the CC) and other assets that may be included in the risk assessment. The CSP should include both hardware and software asset identification.

Threats: Threats and their sources should be identified. Threats may be natural or human-caused, accidental or deliberate, and may be internal or external of the organization. The CCs should focus on threats such as technical failures that affect their information assets, as such threats can be maintained by the CSP. Threats that could be beyond the CSP's scope of responsibility (i.e., threats from within the CC's organization) can be included in their own risk assessment. The CSP should classify the threats sent by the CCs according to their effects on security requirements.

Existing and planned controls: Existing and planned controls should be identified to avoid unnecessary controls and to ensure that existing controls work correctly. The effectiveness of the control can be defined by how it reduces the likelihood of threats and the ease of exploiting the vulnerability. The CCs should evaluate the security controls that affect their information assets and propose additional controls. Other controls, such as physical controls that are beyond the CSP's control, may be included in their own risk assessment. The CSP should review the effectiveness of the CCs' controls and provide more customization of its controls to cover the requirements of CCs.

Vulnerabilities: Vulnerabilities that can be exploited by threats that may harm the assets or the organization should be identified. Usually, a vulnerability has a corresponding threat that may exploit it, unless it poses no risks. The CCs should identify the vulnerabilities that affect their software assets. Some vulnerabilities that are beyond the scope of the CSP's responsibilities, such as personnel or site-related vulnerabilities, can be considered in their self-risk assessment.

Incident consequences: Incidents that compromise data confidentiality, integrity, and availability (or any security objective important to the CC or CSP) as well as their consequences should be identified. The loss of confidentiality may result from an incident that may affect one or more assets. The effect of the incident should be determined by considering the impact criteria defined during the context establishment. The CCs should identify the incidents and the consequences that may affect information assets. The same incidents may have different consequences for different CCs. The CSP should use the list of incidents and consequences to assess the business impact that may result from the security incidents. In addition, the CSP should assess the likelihood of each incident and its consequences by using qualitative or quantitative analysis techniques.

Upon receiving all the lists from the CCs, the CSP will be able to determine the risk level based on the likelihood

of the incident scenario and its consequences. The CSP is responsible for comparing the risk levels with the risk evaluation and risk acceptance criteria. This comparison aims to produce a priority list of risks.

4.3. Risk treatment

When risk assessment is finished, a list of assessed risks, which are prioritized according to the risk evaluation criteria, would be produced. In this phase, the CSP has to implement appropriate security controls to address the risk. Four risk treatment options are available, namely, risk modification, risk retention, risk avoidance, and risk sharing. In the next phase, the CSP would have a risk treatment plan and will identify all residual risks subject to the decision of the organization's managers and the CCs' expectations.

4.4. Risk acceptance

In this phase, the CSP should ensure that the treatment plan has decreased the risk to an acceptable level. The CSP should consider the risk acceptance criteria of the CCs as well as justify risk acceptance decisions and ensure that these risks will not affect its security objective or the CCs' business objective.

4.5. Risk communication and consultation

The clients and the provider must communicate constantly. This communication starts when the CSP notifies the CCs to start context establishment and should continue until the end of the process. The CSP should share information about risks with the CCs. The CSPRAM will send the information to the CCs through the CSP3C. The information includes a report of existing risks, treatment plan, residual risks, and accepted risks. The information sent to the CC must be related to the criteria and expectations. Communication between the CSP and CCs will enable the CSP to understand their security requirements, serve them as group/groups, and communicate with them individually.

4.6. Risk monitoring and review

The CSP should monitor and review the risks and their factors, such as the value of assets, impacts, threats, vulnerabilities, and likelihood of occurrence. Any change in the context must be considered in the next iteration. The CSP is responsible for ensuring consistency between risk management and risk acceptance criteria. Table II summarizes the proposed distribution of the risk assessment tasks between the CCs and the CSP. The "I" in Table I refers to the entity inclusion "included" and "NI" refers to the entity exclusion "not included."

Security risk assessment is an iterative process. Each iteration may take a certain time. In each new iteration, the CC will be able to update the security requirements and evaluate the performance of the security controls imposed by the CSP. In addition, the CSP will also be able to assess the treatment plan and discover potential risks.

Table II. Proposed distribution for the risk assessment tasks between the cloud clients and the communications service provider.

No	Service provider inclusion	Client inclusion	ISO 27005 process tasks
1			• Context establishment
	I	I	• Setting the basic criteria
	I	I	• Scope and boundaries
	I	NI	• Organization for information security risk management
2			• Risk assessment
	I	I	• Risk identification
	I	NI	• Risk analysis (estimation)
	I	NI	• Risk evaluation
3	I	NI	• Risk treatment
4	I	NI	• Risk acceptance
5	I	I	• Risk communication and consultation
6	I	NI	• Risk monitoring and review

I, included; NI, not included; ISO, International Organization for Standardization.

4.7. Initial experiment

In this section, we discuss a scenario in which the proposed framework is used by a SaaS provider to assess security risks. *ABC* is a SaaS provider that offers cloud-based solutions to its clients. One of its products is *PWK*, a website package, which targets medium and small organizations that sell products on the Web. *PWK* offers a hosting service with a website template that can be customized easily for their clients. *PWK* has three different options for the clients that vary according to the amount of storage on the hosting server, allowed bandwidth, number of customizable pages, and database features such as the number of allowed records, categories, and product attributes. The client can customize the template according to his needs by going through a sequence of customization steps.

In this study, we will discuss two of *ABC*'s clients. Client A is a trading company that focuses on electronic devices, and client B is a trading company that focuses on digital music. The customers of client A can explore and buy electronic devices via the Web site, and the company will later deliver the device. The customers of client B can listen to samples of music files, and they can download the complete file immediately upon payment.

When *ABC* decides to start risk assessment, the CSPRAM will notify the clients through the CSP3C to start the context establishment phase. Clients A and B will determine which critical data would be uploaded to the cloud. This data must be categorized on the basis of its importance to the business objectives and its criticality, which is low, medium, or high. Table III shows how clients

Table III. Defining data criticality.

	Data criticality	
Data category	A	B
Users' information	Medium	Medium
Clients' information	Medium	Low
Product information	Low	Medium
Digital commodity	NA	High
Finance transactions	High	High

NA, not applicable.

of the same service may have different evaluations for the same kind of data.

The clients will also define relevant laws. For instance, although clients A and B are both concerned about e-commerce laws, client B is more concerned about copyright laws. Moreover, clients A and B should define their security requirements as well as set criteria for risk acceptance and risk evaluation based on their business objectives and operations. The criteria for risk impact and risk evaluation can be defined according to each client's required security objectives. Table IV shows the clients' identified security requirements. Although the clients use the same software service, their risk criteria will be different because they have different business objectives and data aspects.

The CCs can define general criteria for risk acceptance; for example, they can accept low risk according to the risk analysis matrix shown in Table V [33]. The resulting risk is measured on a scale of 0 to 8 that can be evaluated on the basis of the risk acceptance criteria. This risk scale could also be mapped to a simple overall risk rating: low risk: 0–2, medium risk: 3–5 and high risk: 6–8.

Table IV. Clients' security requirements.

Security requirements			
A		B	
Confidentiality	Medium	Confidentiality	High
Integrity	High	Integrity	High
Availability	High	Availability	High
Identification	High	Identification	High
		Authorization	Medium

All these information will be sent to ABC. Once ABC receives the information, it will define the boundaries and constraints that must be considered and set the basic criteria for risk acceptance, risk impact, and risk evaluation. In addition, ABC will set the risk assessment plan that covers his clients security requirements as well as his own. The service provider must pay more attention to the clients' criteria when it sets the basic criteria for risk acceptance, risk impact, and risk evaluation. The risks that negatively affect any one of the clients' business objectives and business operation must be marked as high risk and subsequently rejected.

Communications service provider may classify CCs into groups according to their security needs. In a same group, the highest security requirement will be applied to the rest of the clients in that group. If two CCs in the same group have different evaluations of the same security objective, the highest evaluation must be considered. For instance, if client A evaluates integrity as medium and client B evaluates integrity objective as high, then integrity must be evaluated as high.

At this point, the *ABC* provider will be able to start the risk assessment process. The CCs will be involved only in the risk identification phase, during which all the risk factors (i.e., assets, threats, vulnerabilities, controls, and incident consequences) must be identified. The clients should be involved in this phase because they are the only ones who know the real value of the company's assets and the consequences that will arise when the security of these assets is compromised. Moreover, the clients may provide a valuable evaluation of the controls imposed by the provider.

The provider will inform the clients to conduct risk identification to identify the risk factors. The clients will identify the assets (i.e., data) or plans that were uploaded on the cloud. The potential value of these assets, the potential threats, and the consequences of compromised security would be defined. If this is not the first phase of the risk assessment, then the client may evaluate the provider's treatment plan and the effectiveness of the controls. Both the CSP and the CCs may apply the suggested methods at ISO27005:2011 annex E to quantify their assessments.

The consequence of lost asset security differs from one client to another. In our example, although client A may be affected by the loss of data confidentiality, he/she will be able to continue his/her business as soon as the problem

Table V. Risk analysis matrix.

	Likelihood of incident scenario				
Business impact	Very low	Low	Medium	High (likely)	Very high
Very low	0	1	2	3	4
Low	1	2	3	4	5
Medium	2	3	4	5	6
High	3	4	5	6	7
Very high	4	5	6	7	8

is solved. However, client B may be affected more negatively because his/her loss may have other consequences. For example, he/she may be accused of violating the copyrights of music, which may have serious legal repercussions. By considering such differences, the provider will be able to identify risk factors with a more realistic consideration of the clients' risk identification.

Thus, the provider will be able to perform risk analysis with more accurate details about the assets, threats, vulnerabilities, and consequences of the incidents. Risk analysis ultimately aims to create a priority list of security risks. The next step for the provider is to evaluate the list of risks, which entail comparing the risk levels with the risk acceptance criteria. The provider must then implement a treatment plan to reduce the risks that are higher than the accepted risk level. Feedback must then be given to the clients. Then, the next iteration of risk assessment may start. During the iterations, the CC will be able to update its assessments and correct any wrongs. Further, the CSP will be able to refine the CCs' security requirments and assessments as well.

5. CONCLUSIONS

Cloud computing offers many economic benefits for IT systems, such as low cost, availability of resources, energy saving, and improved focus on business objectives. However, cloud computing involves many security risks, which may require the re-evaluation of well-known risks based on the cloud computing model. This paper proposes a risk assessment framework for cloud computing, which can be used by service providers, and it involves CCs in the early stages of risk assessment. This framework will enable the cloud service provider to consider changes/updates in the CCs' security objectives. Moreover, the risk assessment results will be more realistic and accurate as the risk factors are defined by all stakeholders. In our future study, we would test, enhance, and refine the proposed framework by testing it with a real SaaS provider.

ACKNOWLEDGEMENT

This work is supported by the Ministry of Higher Education (MOHE), Malaysia and the Research Management Center, Universiti Teknologi Malaysia (UTM) under grant no. 07J92.

REFERENCES

1. Peiyu LIU, Dong LIU. The new risk assessment model for information system in cloud computing environment. *Procedia Engineering* 2011; **15**: 3200–3204.
2. Mell P, Grance T. The NIST definition of cloud computing (draft). *NIST special publication* 800.145, 2011.
3. Michael A, Armando F, Rean G, Anthony D, Randy K, Andy K, *et al*. Above the clouds: a berkeley view of cloud computing. *EECS Department, University of California, Berkeley, Tech. Rep. UCB/EECS-2009-28*, 2009.
4. Saripalli P, Walters B. QUIRC: a quantitative impact and risk assessment framework for cloud security. In *Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on*, 2010; 280–288.
5. Chen Y, Paxson V, Katz RH. What's new about cloud computing security? *University of California, Berkeley Report No. UCB/EECS-2010-5 January*, vol. 20, 2010; 2010–2015.
6. Zissis D, Lekkas D. Addressing cloud computing security issues. *Future Generation Computer Systems* 2012; **28**:583–592.
7. Tanimoto S, Hiramoto M, Iwashita M, Sato H, Kanai A. Risk management on the security problem in cloud computing. In *Computers, Networks, Systems and Industrial Engineering (CNSI), 2011 First ACIS/JNU International Conference on*, 2011; 147–152.
8. Almorsy M, Grundy J, Ibrahim AS. Collaboration-based cloud computing security management framework. In *Cloud Computing (CLOUD), 2011 IEEE International Conference on*, 2011; 364–371.
9. Zhao G. Holistic framework of security management for cloud service providers. In *Industrial Informatics (INDIN), 2012 10th IEEE International Conference on*, 2012; 852–856.
10. Djemame K, Armstrong D, Kiran M, Jiang M. A risk assessment framework and software toolkit for cloud service ecosystems. Presented at the CLOUD COMPUTING 2011, The Second International Conference on Cloud Computing, GRIDs, and Virtualization, 2011.
11. S. NIST. Guide for conducting risk assessments—revision 1. National Institute of Standards and Technology (NIST), 2011.
12. NIST. Managing information security risk: organization, mission, and information system view—SP 800–39. National Institute of Standards and Technology (NIST), 2011.
13. G. o. t. HKSAR. An overview of information security standards. The Government of the Hong Kong Special Administrative Region, 2008.
14. Speake G, Winkler VJR. *Securing the Cloud: Cloud Computer Security Techniques and Tactics*. Rockland, MA, USA: Syngress Publishing, 2011.
15. ISACA. COBIT 5: A business framework for the governance and management of enterprise IT, 2012, 11-5-2012. Available: http://www.isaca.org/cobit/pages/default.aspx.
16. Brodkin J. Gartner: seven cloud-computing security risks. *Infoworld*, 2008; 1–3.
17. ENISA. Cloud computing: benefits, risks and recommendations for information security. The European Network and Information Security Agency (ENISA), 2009.

18. Manavi S, Mohammadalian S, Udzir NI, Abdullah A. Hierarchical secure virtualization model for cloud. In *Cyber Security, Cyber Warfare and Digital Forensic (CyberSec), 2012 International Conference on*, 2012; 219–224.
19. Park JH. A virtualization security framework for public cloud computing. *Computer Science and its Applications* 2012: **203**:421–428.
20. Luo X, Yang L, Ma L, Chu S, Dai H. Virtualization Security risks and solutions of cloud computing via divide-conquer strategy. In *Multimedia Information Networking and Security (MINES), 2011 Third International Conference on*, 2011; 637–641.
21. Lombardi F, Di Pietro R. Secure virtualization for cloud computing. *Journal of Network and Computer Applications* 2011; **34**:1113–1122.
22. Chu CH, Ouyang YC, Jang CB. Secure data transmission with cloud computing in heterogeneous wireless networks. *Security and Communication Networks* 2012; **5**(12): 1325–1336.
23. Morin J, Aubert J, Gateau B. Towards cloud computing SLA risk management: issues and challenges. In *System Science (HICSS), 2012 45th Hawaii International Conference on*, 2012; 5509–5514.
24. Hammadi AM, Hussain O. A framework for SLA assurance in cloud computing. In *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*, 2012; 393–398.
25. Yan W, Ansari N. Anti-virus in-the-cloud service: are we ready for the security evolution? *Security and Communication Networks* 2011; **5**:572–582.
26. Khorshed MT, Ali A, Wasimi SA. Classifying different denial-of-service attacks in cloud computing using rule-based learning. *Security and Communication Networks* 2012.
27. Wang B, Huang He Y, Liu Xiao X, Jing MX. Open identity management framework for SaaS ecosystem. In *e-Business Engineering, 2009. ICEBE '09. IEEE International Conference on*, 2009; 512–517.
28. Xuan Z, Wuwong N, Hao L, Xuejie Z. Information security risk management framework for the cloud computing environments. In *Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on*, 2010; 1328–1334.
29. Fito JO, Guitart J. Business-driven management of infrastructure-level risks in Cloud providers. *Future Generation Computer Systems* 2012.
30. Fito JO, Macias M, Guitart J. Toward business-driven risk management for Cloud computing. In *Network and Service Management (CNSM), 2010 International Conference on*, 2010; 238–241.
31. FERMA. FERMA's—a risk management standard, 2003, 30-08-2012. Available: http://www.ferma.eu/risk-management/standards/risk-management-standard/.
32. Landoll DJ. *The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments* (Second edn). CRC Press Taylor & Francis Group; 6000 Broken Sound Parkway NW, Suite 300 Boca Raton, FL 33487-2742, 2011.
33. British.Standard. Information technology—security techniques—information security risk management ed. Switzerland: British Standard, 2011.